

DETAILED ACTION

- I. Claims 1-14 have been examined.

Claim Rejections - 35 USC § 102

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-4, 6, 7, 9, 12 and 14 are rejected under 35 U.S.C. 102(e) as being anticipated by United States Patent No. 6,501,956 to Weeren et al., hereinafter Weeren.

1. Regarding claim 1, Weeren teaches a method of enabling a multitasking computing device to preserve system resources, comprising the steps of determining if an untrusted application is in the background or foreground and preventing an untrusted application that is in the background from running (column 4, lines 6-11, "the data application may then be suspended until the telephony session terminates" and lines 29-54, "As the telecommunication link is suspended or terminated, the data application is brought back to the foreground, such as by reactivation or redesignation as the active task, to operate with the user").

[The Applicant defines the "untrusted application" to pertain to, inter alia, "applications which are from certain kinds of third party programmers". Said "untrusted application" is interpreted by the Examiner to pertain to the "data application" disclosed within Weeren (e.g. column 4, lines 37-44, "A wireless data application generator, which can be a WML page generator, an HDML page generator, or some other wireless data application language, builds the data

application information in a format compatible with the mobile communication device and wireless data network").]

2. Regarding claim 2, Weeren teaches in which a window server component determines if the untrusted application is in the background or foreground (column 4, lines 29-36 and 48-54, "Other situations may result in an automatic push of the data to the communication device when the data application is operating in the foreground").

3. Regarding claim 3, Weeren teaches in which, for an untrusted application in the background, the window server sends a control signal to a scheduler or interrupt handler to prevent the application from running (column 4, lines 6-11, "the data application may then be suspended until the telephony session terminates").

4. Regarding claim 4, Weeren teaches the further step of preventing an untrusted background application from 'polling' for data over a wireless network (column 4, lines 29-36, "the telecommunication link is suspended or terminated").

[With the "link" no longer having an established connection, data cannot be obtained over the "wireless network".]

5. Regarding claim 6, Weeren teaches in which a trusted application in the background is (i) still allowed to run, or (ii) actively prevented from running or (III) requested to stop running (column 7, lines 37-47, column 11, lines 58-67 and column 12, lines 1-23).

6. Regarding claim 7, Weeren teaches in which an application has been deemed to be untrusted by the device assessing: (a) which protected resources on the device can be accessed by the application; or (b) whether the application was loaded from ROM or

RAM; or (c) whether the application has been validated using some predefined validation or certification process (column 9, lines 55-67, "The indefinitely permanent memory location..." and column 10, lines 1-12, "stored information will preferably remain in Data Store 24 until deleted by the user or by the network provider, in accordance with any service contract provisions").

7. Regarding claim 9, Weeren teaches in which the device is battery powered (Figures 1a, 1b and 2, element 1000, column 6, lines 13-37, "mobile device 1000 in Cellular/Wireless System 10").

[As it is known, a mobile device/cellular phone is powered by a battery.]

8. Regarding claim 12, Weeren discloses a multitasking computing device programmed to be capable of determining if an untrusted application is in the background or foreground and preventing an untrusted application that is in the background from running in order to conserve system resources (column 4, lines 6-11, "the data application may then be suspended until the telephony session terminates" and lines 29-54, "As the telecommunication link is suspended or terminated, the data application is brought back to the foreground, such as by reactivation or redesignation as the active task, to operate with the user").

[The Applicant defines the "untrusted application" to pertain to, inter alia, "applications which are from certain kinds of third party programmers". Said "untrusted application" is interpreted by the Examiner to pertain to the "data application" disclosed within Weeren (e.g. column 4, lines 37-44, "A wireless data application generator, which can be a WML page generator, an HTML page

generator, or some other wireless data application language, builds the data application information in a format compatible with the mobile communication device and wireless data network").]

9. Regarding claim 14, Weeren discloses an operating system for a multitasking computing device, the operating system being capable of determining if an untrusted application is in the background or foreground and preventing an untrusted application that is in the background from running in order to conserve system resources (column 4, lines 6-11, "the data application may then be suspended until the telephony session terminates" and lines 29-54, "As the telecommunication link is suspended or terminated, the data application is brought back to the foreground, such as by reactivation or redesignation as the active task, to operate with the user").

[The Applicant defines the "untrusted application" to pertain to, inter alia, "applications which are from certain kinds of third party programmers". Said "untrusted application" is interpreted by the Examiner to pertain to the "data application" disclosed within Weeren (e.g. column 4, lines 37-44, "A wireless data application generator, which can be a WML page generator, an HDML page generator, or some other wireless data application language, builds the data application information in a format compatible with the mobile communication device and wireless data network").]

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148

USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 5, 8, 10, 11 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Weeren as applied to claim 1 above, and further in view of United States Patent No. 6,014,746 to Krehnke et al., hereinafter Krehnke.

10. Weeren teaches the claimed invention, as cited above. However, Weeren does not substantially teach the claim language within claims 5, 8, 10 and 11. Krehnke teaches said claim language, as cited below.

11. Regarding claim 5, Krehnke teaches the further step of preventing an untrusted background application from running if a display shows a screen saver or is turned off (column 3, lines 41-44, "the armed state screen occludes data from any application(s) working in background mode" and column 8, lines 2-4).

12. The motivation to combine would be to prevent any intruders from obtaining information via attempting to view it on the display screen of the device(s) (see column 3, lines 41-44 for support for this motivation).

13. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Krehnke with the teachings of Weeren to either have the display screen become blank or have a particular image on said screen in order to obscure the viewing of any pertinent data from unauthorized personnel.

14. Regarding claim 8, Krehnke teaches in which a background application is prevented from running only if it does not meet predefined 'trust' or certification criteria established using a signature in an installation file for the application (column 4, lines 24-36, column 7, lines 59-64 and column 8, lines 44-52).

15. The motivation to combine would be to detect any changes within the file(s) and prevent any tampering or other harmful practices from occurring on the device(s). (refer to column 4, lines 24-36 of Krehnke for support of this motivation).

16. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Krehnke with the teachings of Weeren so that the data within the device(s) can be securely monitored and the appropriate user(s) or authorities can be promptly notified if there is any compromise in the integrity of the data processes; thus maintaining a level of protection for the device(s) and processes therein.

17. Regarding claim 10, Krehnke teaches in which the system resources that are preserved are *one or more of* (i) power, (ii) CPU activity and (iii) scheduler activity (column 3, lines 17-22 and column 8, lines 11-17).

18. The motivation to combine would be to only utilize the appropriate resources at the appropriate time(s) so as to not exhaust the power source for the device(s) (refer to column 8, lines 11-17 of Krehnke for support for this motivation).

19. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Krehnke within the teachings of Weeren to have a configuration in which power can be utilized for the security measures of the device but on a temporary basis and not be a drain on the power source when said measures would not be needed to be utilized to their full capacity.

20. Regarding claim 11, Krehnke teaches in which the device is powered by a UPS (uninterruptible power supply) (column 7, lines 29-35, "contains a battery backup that continues to drive a 100 db alarm even if power on the PC is interrupted").

[As it is known, a UPS is a battery back-up; thus Krehnke discloses the claimed "UPS (uninterruptible power supply)".]

21. The motivation to combine would be to have a security mechanism which cannot be thwarted by a loss of power (refer to column 3, lines 7-16 of Krehnke for support of this motivation).

22. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Krehnke with the teachings of Weeren in order to have a battery back-up to compensate for an interrupt in power in order to preserve the integrity and security of the device(s).

23. Though Weeren discloses the claim language within claim 13, by virtue of its dependency upon claim 11, it is hereby rejected under 35 U.S.C. 103(a).
24. Regarding claim 13, Weeren discloses the device of claim 11 which is battery powered (Figures 1a, 1b and 2, element 1000, column 6, lines 13-37, "mobile device 1000 in Cellular/Wireless System 10").

[As it is known, a mobile device/cellular phone is powered by a battery.]

Conclusion

25. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.
26. The following United States Patents are cited to further show the state of the art with respect to proper resource access, such as:

United States Patent No. 6,011,537 to Slotznick, which is cited to show a system for delivering and simultaneously displaying primary and secondary information, and for displaying only the secondary information during interstitial space.

United States Patent No. 7,069,586 to Winneg et al., which is cited to show securely executing an application on a computer system.

United States Patent No. 7,275,177 to Armangau et al., which is cited to show data recovery with internet protocol replication with or without full resync.

United States Patent No. 5,046,082 to Zicker et al., which is cited to show a remote accessing system for cellular telephones.

United States Patent No. 7,015,817 to Copley et al., which is cited to show a personal tracking device.

United States Patent No. 7,382,773 to Schoeneberger et al. which is cited to show a contact center with normalized multiple protocol architecture.

27. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEREMIAH AVERY whose telephone number is (571)272-8627. The examiner can normally be reached on Monday thru Friday 8:30am-5pm.

28. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

29. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Jeremiah Avery/
Examiner, Art Unit 2431

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431